IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	)	Criminal No. 8:21-CR-21 (MAD)
	)	
v.	)	**Plea Agreement**
	)	
NICHOLAS FABER,	)	
	)	
	)	
Defendant.	)	

The United States of America, by and through its counsel of record, the United States Attorney for the Northern District of New York, and defendant **NICHOLAS FABER** (hereinafter "the defendant"), by and through the defendant's counsel of record, hereby enter into the following plea agreement pursuant to Rule 11(c)(1)(A) of the Federal Rules of Criminal Procedure:

1) **The Defendant's Obligations:**

a) **Guilty Plea:** The defendant will plead guilty to Counts One and Two of the Information in Case No. 8:21-CR-21 (MAD) charging one count of Computer Intrusion Causing Damage, in violation of 18 U.S.C. § 1030(a)(5)(A), and one count of Aggravated Identity Theft, in violation of 18 U.S.C. § 1028A.

b) **Special Assessment:** The defendant will pay an assessment of $100 per count of conviction pursuant to 18 U.S.C. § 3013. The defendant agrees to deliver a check or money order to the Clerk of the Court in the amount of $200, payable to the U.S. District Court, at the time of sentencing.

c) **Compliance with Other Terms of Agreement:** The defendant will comply in a timely manner with all of the terms of this plea agreement.

d) **Restitution:** The defendant will consent to entry of an order directing the defendant's payment of restitution in the amount of $35,430.85 to the State University of New York at

Plattsburgh, whether or not the losses suffered by the victim resulted from the offenses of conviction.

e) **Forfeiture:** Pursuant to § 1030(i)(1)(A) and 21 U.S.C. § 853(p), the defendant will consent to entry of an order directing forfeiture to the United States of the property described in the Forfeiture Allegation in the Information described above, or to any substitute assets, or to a money judgment, all as more fully set out below:

1) Black iPhone X Model: MRYR2LL/A; Serial Number: FK1XLAL5KXKN
2) MacBook Pro with black case; Serial Number: FVFVV89RHV22
3) HP Elite Book laptop; Windows product key 89QF8-4NBMB-8HMWDW-YP2HG
4) MacBook Pro laptop; Serial Number: C0ZQNDUIFVH3
5) Five USB flash drives
    a) Model: SDCZ6-1024; Serial Number: BB0806KOIB
    b) Model: SDCZ6-4096RB; Serial Number: BH0809NRCB
    c) No outer shell. Internal Serial Number: AAP6WFQ9WIA1E11M
    d) Model: SDCZ60-016g; Serial Number (partial): BL1702252
    e) Internal Serial Number: 6C680E13
6) Insignia tablet Model: NS-15T8LTE; Serial Number: 14J05A012861
7) iPad (silver), J303—L3Z38
8) iPhone, model A1549 (silver)

If any of the property described above, as a result of any act or omission of the defendant, either: (a) cannot be located upon the exercise of due diligence; (b) has been transferred or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the court; (d) has been substantially diminished in value; or (e) has been commingled with

other property which cannot be divided without difficulty, the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p) and Fed. R. Crim. P. 32.2(e).

2) **The Government's Obligations:**

a) **Non-prosecution for other offenses:** For so long as the defendant's guilty plea and the sentence remain in effect, the government will not seek other federal criminal charges against the defendant based on conduct described in the Information in Case No. 8:21-CR-21 (MAD) and/or in the paragraph of this agreement entitled "Factual Basis for Guilty Plea," occurring before the date on which the defendant signs this agreement. This agreement does not prevent the government from seeking charges based on other conduct.

b) **Compliance with Other Terms of Agreement:** The government will comply in a timely manner with all of the terms of this plea agreement.

3) **Potential Maximum Penalties:** The defendant understands that the Court can impose the following maximum penalties for the offenses to which the defendant agrees to plead guilty and may be required to impose mandatory minimum terms of imprisonment, all as set out below:

Count One: Computer Intrusion Causing Damage

a) **Maximum term of imprisonment:** ten years, pursuant to 18 U.S.C. § 1030(c)(4)(B)(i).

b) **Maximum fine:** $250,000, pursuant to 18 U.S.C. § 3571.

Count Two: Aggravated Identity Theft

a) **Maximum term of imprisonment:** two years, pursuant to 18 U.S.C. § 1028A(a)(1). The term of imprisonment is mandatory and must be served consecutively with any other sentence of imprisonment.

b) **Maximum fine:** $250,000, pursuant to 18 U.S.C. § 3571(b)(3).

All Counts

a) **Supervised release term:** In addition to imposing any other penalty, the sentencing court may require the defendant to serve a term of supervised release of up to three years, to begin after imprisonment. *See* 18 U.S.C. § 3583. A violation of the conditions of supervised release during that time period may result in the defendant being sentenced to an additional term of imprisonment of up to two years.

b) **Other adverse consequences:** Other adverse consequences may result from the defendant's guilty plea as further described in paragraph F below.

4) **Elements of Offenses:** The defendant understands that the following are the elements of the offenses to which the defendant agrees to plead guilty.

Count One: Computer Intrusion Causing Damage

a) ***First,*** that the defendant knowingly caused the transmission of a program, information, code, or a command to a protected computer;

b) ***Second,*** as a result of such conduct, the defendant intentionally caused damage to a protected computer without authorization; and

c) ***Third,*** the offense caused loss to a person during a one-year period aggregating at least $5,000 in value.

Count Two: Aggravated Identity Theft

a) ***First,*** the defendant knowingly transferred, possessed, or used a means of identification of another person;

b) ***Second,*** the defendant did so without lawful authority; and

c) ***Third,*** the defendant did so during and in relation to the qualifying predicate offense of computer fraud, in violation of 18 U.S.C. § 1030(a)(5)(A), as alleged in Count One of the Information.

5) **Factual Basis for Guilty Plea:** The defendant admits the following facts, that those facts demonstrate the defendant's guilt for the offenses to which the defendant is pleading guilty, and that there are no facts establishing any viable defenses to those offenses:

a) Starting at least as early as 2017, when the defendant was a student at State University of New York at Plattsburgh ("SUNY-PB"), he communicated with individuals online that he understood were accessing online accounts of college-age females and stealing their nude photographs and videos. He also identified, by name, those females whose stolen materials he possessed and was willing to trade. The defendant solicited and received such stolen nude materials of specific women, some of whom he knew personally. The defendant received, *inter alia*, more than a dozen stolen, nude photographs of a female with whom he attended high school.

b) The defendant requested others to access specific females' online accounts in order to steal nude photographs and videos the defendant wanted to see. In some instances, the defendant would supply an e-mail address or username of an account he wanted another individual to attempt to break into. The defendant requested others to break into more than 50 online accounts. He received nude photographs and videos from multiple accounts he had directed be accessed and assisted in obtaining access without authorization.

c) The defendant also himself attempted to access more than two dozen accounts of females he knew and successfully accessed approximately ten accounts without authorization.

When he successfully accessed online accounts, he looked for and stole any nude photographs or videos he found and traded the stolen materials with others online.

d) When the defendant attempted to access females' online accounts, he used a virtual private network service in an attempt to conceal his activity and avoid being caught.

e) In or around September 2018, the defendant and another individual ("Individual 1") who was located in the Northern District of New York at all relevant times, discussed online having access to photographs and videos (i.e., "wins") stolen from the online accounts of female college students, including "a lot of [Plattsburgh State University] girls." The defendant and Individual 1 discussed trading the photographs and videos of females, identified by first and last name. In these discussions, the defendant expressed a preference for "new" photographs and videos of "athletes."

f) On or about November 27, 2018, the defendant and Individual 1 exchanged messages online. Individual 1 explained that he had lost his prior unauthorized access to GroupMe chats among a group of sorority women because the woman whose account to which Individual 1 had had unauthorized access had changed her password. The defendant responded "We can try getting into another." The defendant and Individual 1 then discussed ways to access college females' online accounts without authorization by resetting passwords, including the password to "school email."

g) After the conversation above, including on or about November 27, 20218 and December 28, 2018, Individual 1, while in the Northern District of New York, logged into and reset the passwords for female student accounts (including student A.V.) at SUNY-PB, a public university located in Plattsburgh, New York, in the Northern District of New York. The defendant knew that, pursuant to their agreement, Individual 1 was accessing accounts

stored on Internet-connected computers in the Northern District of New York and owned by females attending school at SUNY-PB in the Northern District of New York, including A.V.

h) SUNY-PB has an Internet-connected computer network ("the network") that its students and employees use for educational, commercial, and business purposes. The network is comprised of computer servers and other computer hardware located on the SUNY-PB campus and elsewhere. The computers in SUNY-PB's network facilitate and affect interstate commerce.

i) SUNY-PB assigns network user accounts ("accounts") to access the network to SUNY-PB students. SUNY-PB students can access their accounts over the Internet or by accessing the network directly while on campus. Accessing an account on the network from any location, including the Internet, requires interfacing with computers located on the SUNY-PB campus.

j) To access the network, a SUNY-PB student must enter his or her username (typically, an abbreviated version of the student's name) in conjunction with a user-specified password. Upon accessing the network using these credentials, a SUNY-PB student can then access different types of information. Accessing a typical account would provide access to an online portal, "MyPlattsburgh," containing full access to the student's SUNY-PB email, a cloud storage account (containing, e.g., documents, pictures, videos, etc.), a profile containing biographical information and other personal information, billing and financial aid information, coursework, grades, and other personal information.

k) Individual 1 accessed the SUNY-PB accounts by entering the correct username and password combination, *i.e.*, a means of identification as that term is defined at 18 U.S.C. §

1028(d)(7), into the network. Individual 1 obtained the passwords for these accounts through a variety of means, including using SUNY-PB's password reset function, which allowed an account holder to create a new password by entering the account holder's username into the SUNY-PB website and then correctly answering previously established security questions.

l) Individual 1 accessed these accounts as the defendant advised to browse their content and obtain personal information that he and the defendant could then use to gain access to other online accounts owned by the account holders, such as Snapchat, Facebook, Google, and iCloud, in order to download nude, sexually explicit, and personally embarrassing photographs and videos stored in those other online accounts. The defendant and Individual 1 then traded these stolen photographs and videos with one another and others online.

m) The defendant created and he and Individual 1 then distributed collages that placed some of those stolen nude photographs alongside innocuous photographs of the students (e.g., a private masturbation photograph placed alongside a formal graduation photograph).

n) Because of the defendant's and Individual 1's actions, SUNY-PB sustained a monetary loss, within one year, of more than $5,000. Specifically, between April 2018 and April 2019, SUNY-PB spent at least $35,430.85 investigating and remedying account "lock outs" caused by the unauthorized password resets, implementing measures to prevent the defendant's co-conspirator from accessing the network through virtual private networks, conducting a damage assessment, notifying victims, consulting with experts and attorneys, and restoring compromised data.

o) On or about January 12, 2019, the defendant asked Individual 1 "Hey man any snapchats you want me to try to get into?" and told Individual 1 that he will ask a friend "how he does it if you wanted to try." The defendant then explained that "Basically he texts them off a fake number with some story of how he accidentally signed up for snap with their phone number, and needs a code to change it. Then they give him the code which really lets him reset their PW." The defendant further cautioned Individual 1,"if you do sorority girls you gotta do it smart cause they talk. You know?" and then advised, "I need phone number and snap name." Individual 1 reported, "ive gotten into a few girls snaps U can do it if theyre email is linked to their plattsburhg one, u just answer their security qs" and Individual 1 names two women whose accounts he accessed. After Individual 1 shared a photograph, the defendant responded, "Damn bro good shit! So you think it'd be worth it to try n get into more?" The defendant later reported, "Update: Snapchat changed how his method works. Didn't work . . . The girls used to give the code to him. Now they changed it so it's more like two step verification."

p) In December of 2019, the defendant searched an online list of compromised passwords to find credentials for a female classmate's online account. The defendant accessed the woman's account without authorization but did not find any nude photographs or videos in the part of the account he was able to access. He discovered that a more private part of the account required an additional password that he did not have. The defendant attempted to guess the additional password several times, but failed to guess it correctly.

6) **<u>Sentencing Stipulations:</u>**

Count One: Computer Intrusion Causing Damage

a) The parties agree that the base offense level for Count One is six, pursuant to U.S.S.G. § 2B1.1(a)(2).

b) The parties agree that the loss amount for Count One, attributable to the defendant, is between $6,500 and $15,000, resulting in a two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(1)(B).

c) The parties agree that the offense involved more than ten victims, resulting in a two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(i).

d) The parties agree that the offense involved sophisticated means, resulting in a two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(10).

e) The parties agree that the offense involved an intent to obtain personal information, resulting in a two-level increase, pursuant to U.S.S.G. § 2B1.1(b)(18).

f) The parties agree that the defendant was convicted of an offense under 18 U.S.C. § 1030(a)(5)(A), resulting in a four-level increase, pursuant to U.S.S.G. § 2B1.1(b)(19)(A)(ii).

g) It is the defendant's position that he should receive a mitigating role reduction, pursuant to U.S.S.G. § 3B1.2. It is the government's position that the defendant should not receive a mitigating role reduction.

Count Two: Aggravated Identity Theft

h) The parties agree that the guideline sentence for Count Two is the mandatory sentence under 18 U.S.C. § 1028A(a)(1), *i.e.*, a consecutive 24 month term of imprisonment.

All Counts

i) The government will recommend a 2-level downward adjustment to the applicable federal sentencing guidelines offense level pursuant to U.S.S.G. §3E1.1(a) if, (i) through the time

of sentencing, the government is convinced that the defendant has demonstrated "acceptance of responsibility" for the offenses to which the defendant is pleading guilty and all relevant conduct, as defined in U.S.S.G. § 1B1.3; and (ii) the government does not determine that the defendant, after signing this agreement, committed any other federal, state, or local crimes, or engaged in conduct that constitutes "obstruction of justice," as defined in U.S.S.G. § 3C1.1.

j) The government will move for a 1-level downward adjustment to the applicable federal sentencing guidelines offense level pursuant to U.S.S.G. §3E1.1(b) if the government is convinced that the defendant has accepted responsibility within the meaning of U.S.S.G. §3E1.1(a) and further assisted authorities in the investigation or prosecution of the defendant's own misconduct by timely notifying authorities of the defendant's intention to enter a plea of guilty, thereby permitting the government to avoid preparing for trial and permitting the government and the court to allocate their resources efficiently, and the defendant otherwise qualifies for such adjustment by having a combined offense level of 16 or more before receipt of any acceptance of responsibility adjustment under U.S.S.G. § 3E1.1(a).

7) **Waiver of Rights to Appeal and Collateral Attack:** The defendant waives (gives up) any and all rights, including those conferred by 18 U.S.C. § 3742 and/or 28 U.S.C. §§ 2241 and 2255, to appeal and/or to collaterally attack the following (except that the defendant does not waive the right to raise a claim based on alleged ineffective assistance of counsel):

a) The convictions resulting from the defendant's guilty plea;

b) Any claim that the statutes to which the defendant is pleading guilty is unconstitutional;

c) Any claim that the admitted conduct does not fall within the scope of the statute;

d) Any sentence to a term of imprisonment of 74 months or less;

e) Any sentence to a fine within the maximum permitted by law;

f) Any sentence to a term of supervised release within the maximum permitted by law;

g) Any order of forfeiture or restitution imposed by the Court that is consistent with governing law and is not contrary to the terms of this agreement.

Nothing in this appeal waiver is meant to be or should be construed as a representation of or agreement concerning the appropriate sentence in this case.

NICHOLAS MCQUAID
Acting Assistant Attorney General
Criminal Division

By: /s/ Michael J. Stawasz
Michael J. Stawasz
Deputy Chief for Computer Crime

Dated: 2/5/21

ANTOINETTE T. BACON
Acting United States Attorney
Northern District of New York

By: /s/ Wayne A. Myers
Wayne A. Myers
Assistant United States Attorney
Bar Roll No. 517962

Dated: 2/5/21

Nicholas Faber
Defendant

Dated: 1/25/21

James Wolford, Esq.
Attorney for Defendant
Bar Roll. No. 518326

Dated: 1/25/2021